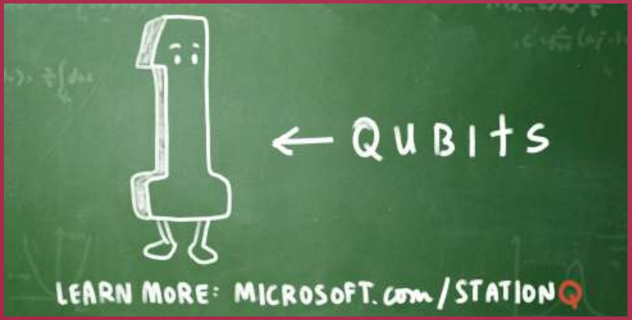
(ALMOST) ALL THERE IS TO KNOW ABOUT QUANTUM CRYPTOGRAPHY

André Souto



LASIGE reliable software systems

ULISBOA   Ciências ULisboa   FCT Fundação para a Ciência e a Tecnologia

ROAD MAP

LASIGE reliable software systems

- Breaking news on quantum computation
- Quantum basics
- Quantum devices
- Quantum in the “zoo”
- Where can we find/use quantum computation
- Cryptographic application
  - Oblivious transfer and bit commitment
  - Why and how
  - Drawbacks and challenges
  - Our approach
- Conclusions and what comes next

BREAKING NEWS ON QUANTUM

reliable
software systems

New algorithm optimizes quantum computing problem-solving

Tohoku University researchers have developed an algorithm that enhances the ability of a Canadian-designed quantum computer to more efficiently find the best solution for complicated problems, according to a study published ...

QUANTUM PHYSICS — APR 10, 2019 — 1 — 210

Quantum simulation more stable than expected

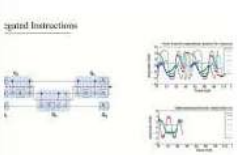
A localization phenomenon boosts the accuracy of solving quantum many-body problems with quantum computers. These problems are otherwise challenging for conventional computers. This brings such digital quantum simulation ...

QUANTUM PHYSICS — APR 12, 2019 — 0 — 1354

Research team expands quantum network with successful long-distance entanglement experiment

Scientists from the U.S. Department of Energy's Brookhaven National Laboratory, Stony Brook University, and DOE's Energy Sciences Network (ESnet) are collaborating on an experiment that puts U.S. quantum networking research ...

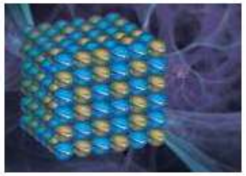
QUANTUM PHYSICS — APR 08, 2019 — 1 — 326



Research provides speed boost to quantum computers

A new finding by researchers at the University of Chicago promises to improve the speed and reliability of current and next generation quantum computers by as much as ten times. By combining principles from physics and computer ...

QUANTUM PHYSICS — APR 12, 2019 — 0 — 348



The spin doctors: Researchers discover surprising quantum effect in hard disk drive material

Scientists find surprising way to affect information storage properties in metal alloy.

QUANTUM PHYSICS — APR 25, 2019 — 1 — 912

Computer program developed to find 'leakage' in quantum computers

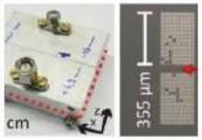
A new computer program that spots when information in a quantum computer is escaping to unwanted states will give users of this promising technology the ability to check its reliability without any technical knowledge for ...

QUANTUM PHYSICS — MAR 19, 2019 — 0 — 770

Implementing a practical quantum secure direct communication system

Quantum secure direct communication (QSDC) is an important branch of quantum communication, based on the principles of quantum mechanics for the direct transmission of classified information. While recent proof-of-principle ...

QUANTUM PHYSICS — feature — FEB 18, 2019 — 0 — 570



Compact 3-D quantum memory addresses long-standing tradeoff

Physicists have designed a 3-D quantum memory that addresses the tradeoff between achieving long storage times and fast readout times, while at the same time maintaining a compact form. The new memory has potential applications ...

QUANTUM PHYSICS — feature — JUN 04, 2018 — 0 — 193

QUANTUM BASICS

- How do we represent information?

QUANTUM BASICS

Classically – using bits! Either 0 or 1

 **or** 

QUANTUM BASICS

Quantumly – using quantum bits!

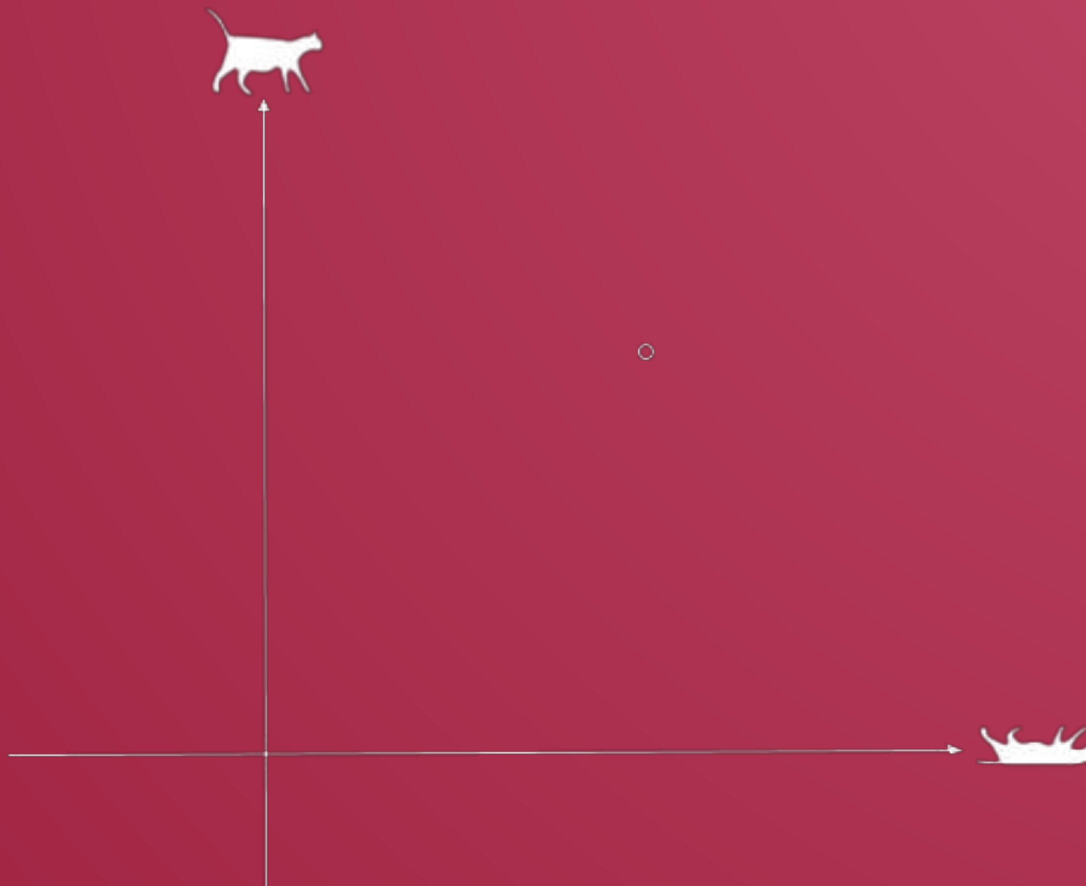
QUANTUM BASICS

Quantumly – using quantum bits!

- 0 and 1, i.e., it can be in any combination of the two!

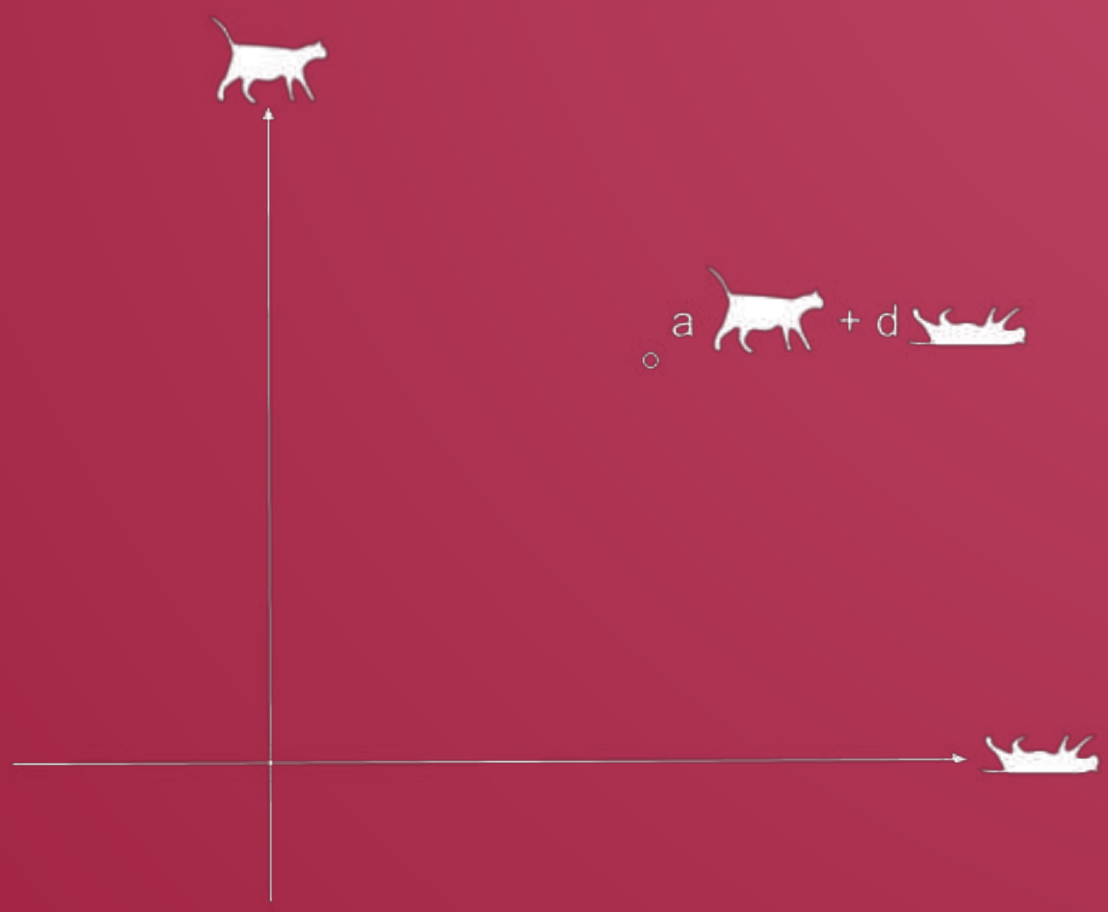
QUANTUM BASICS

LASIGE reliable software systems



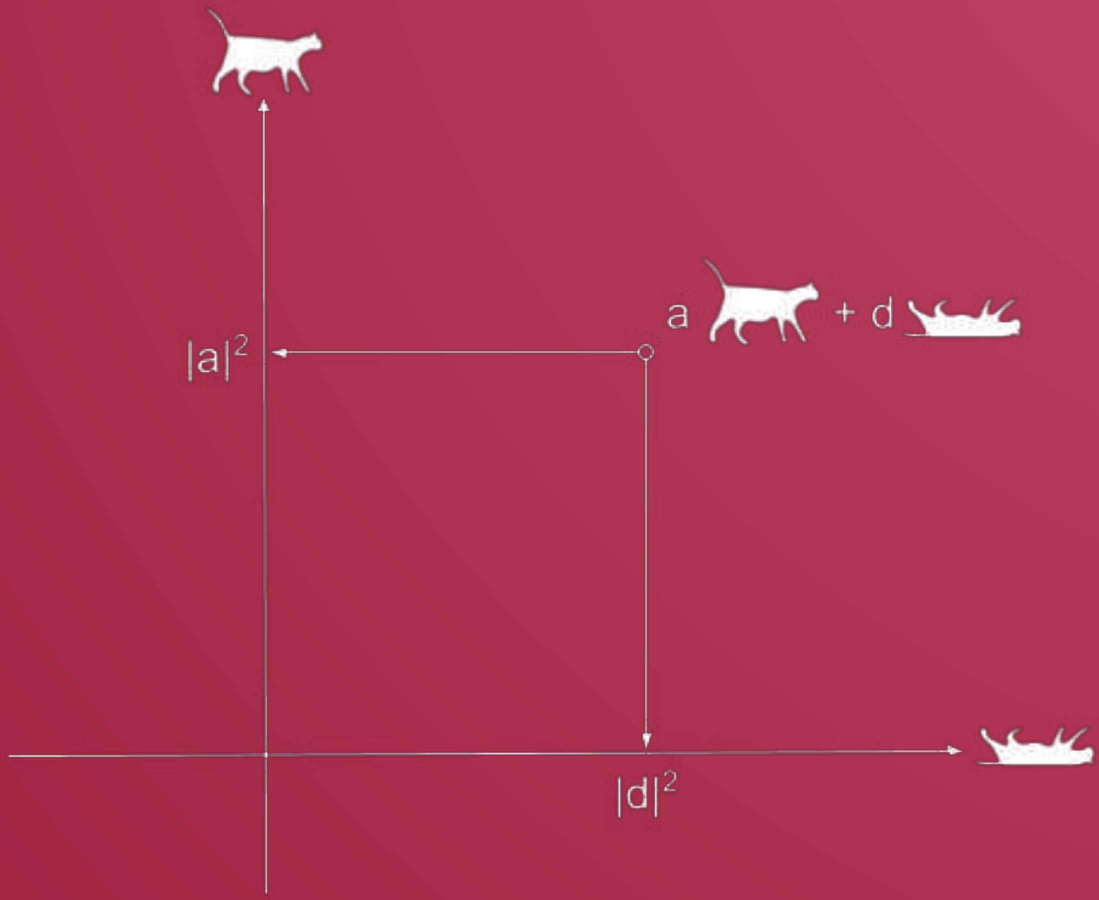
QUANTUM BASICS

LASIGE
reliable software systems



U LISBOA
Ciências ULisboa
FCT Fundação para a Ciência e a Tecnologia

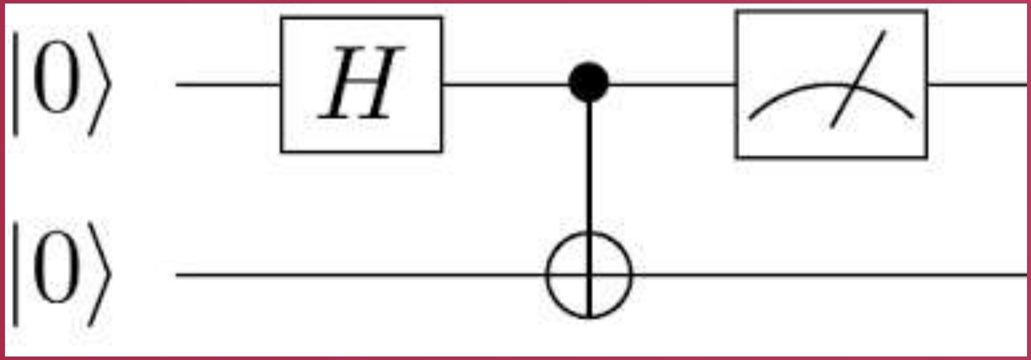
QUANTUM BASICS



QUANTUM BASICS

LASIGE reliable software systems

- The operations for quantum evolution is made by **linear unitary operators** (simple linear algebra!) like C-not, **Hadamard**, QFT CCNOT (Toffoli gate);

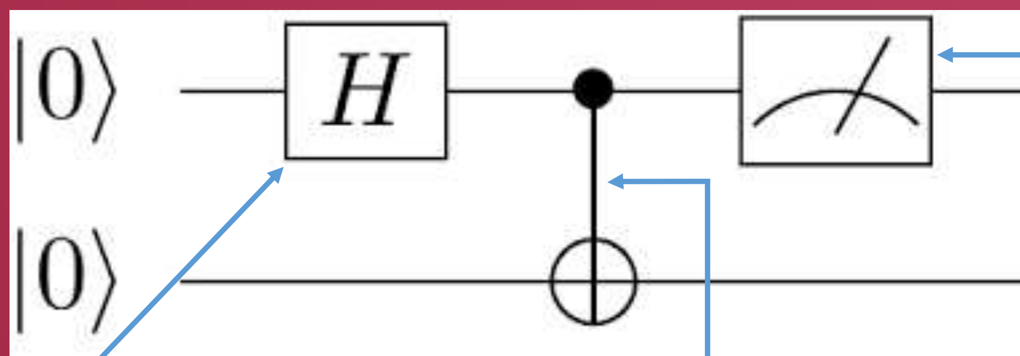


ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

QUANTUM BASICS

LASIGE reliable software systems

- The operations for quantum evolution is made by **linear unitary operators** (simple linear algebra!) like C-not, **Hadamard**, QFT, CCNOT (Toffoli gate);



$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 \\ 1 & -1\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0\end{bmatrix}$$

Measurement (not a quantum op. - irreversible) that gives classical information 0 or 1

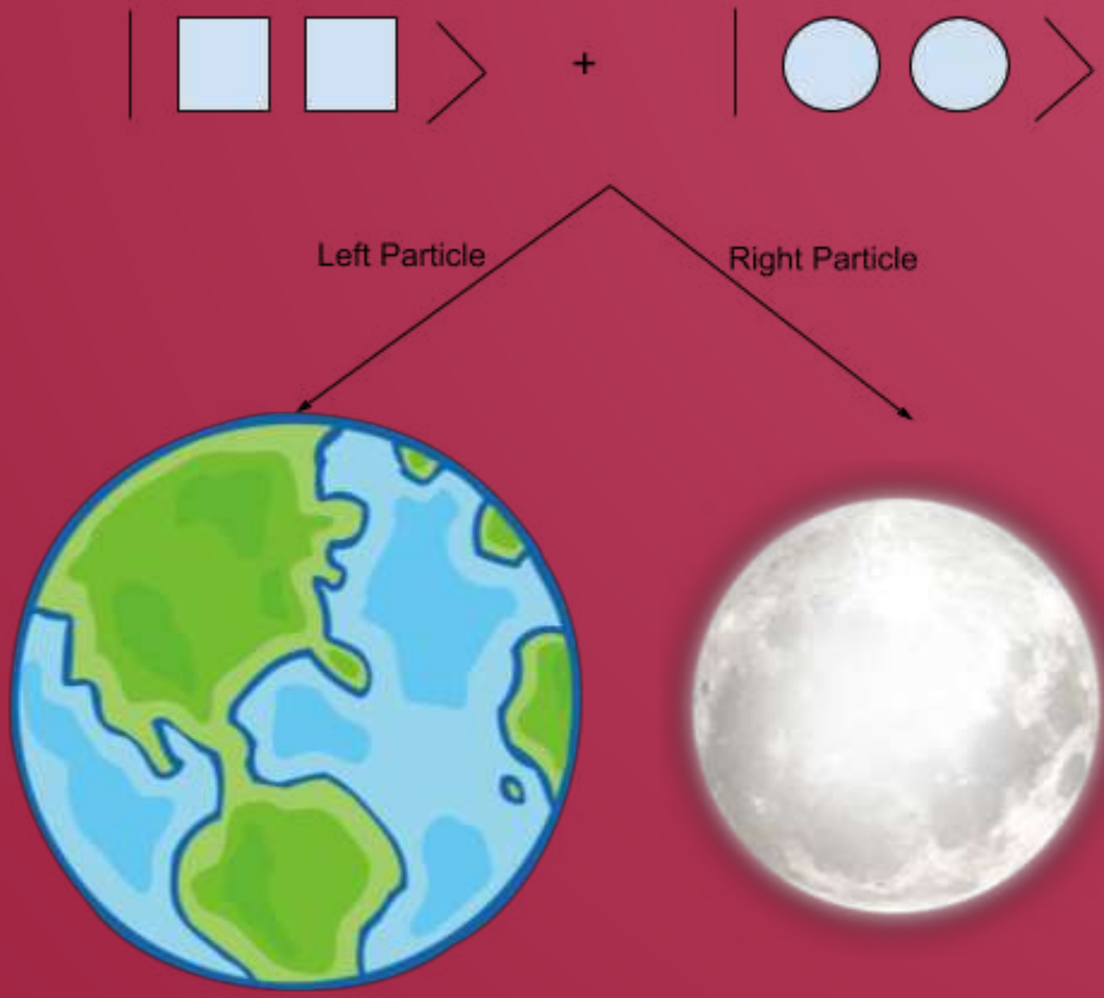
ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

QUANTUM ENTANGLEMENT

LASIGE reliable software systems

U LISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

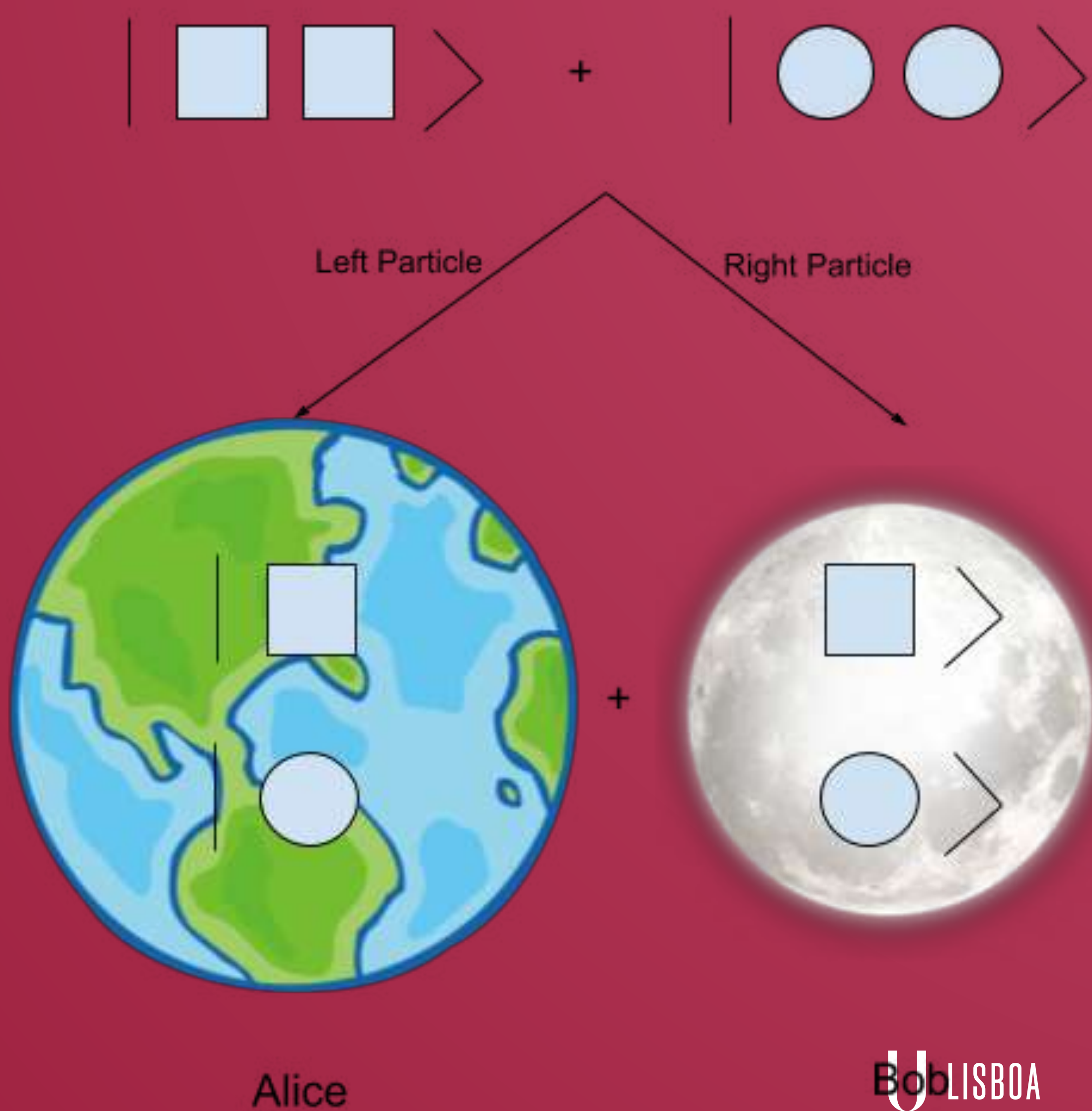
QUANTUM ENTANGLEMENT



Alice

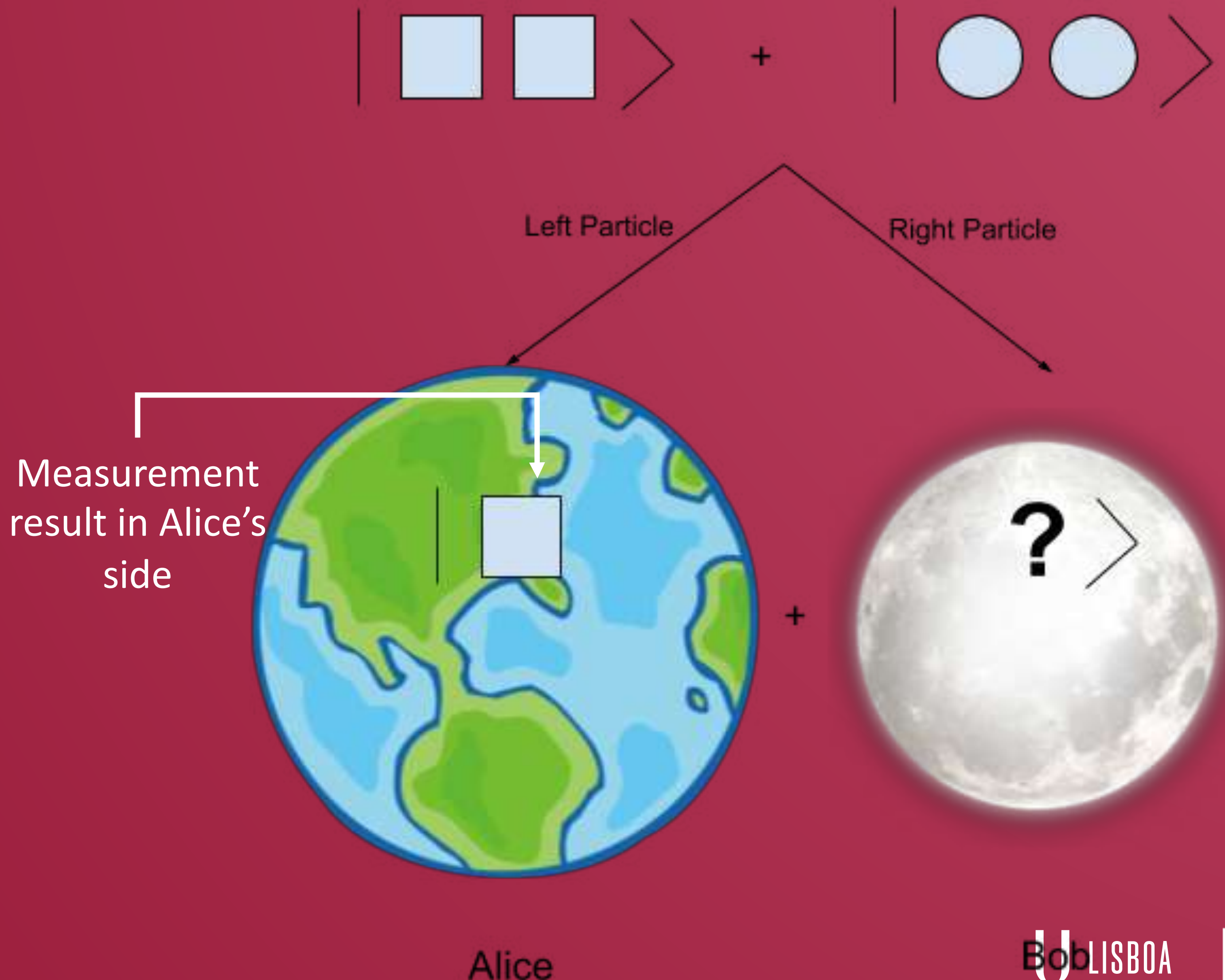
Bob

QUANTUM ENTANGLEMENT



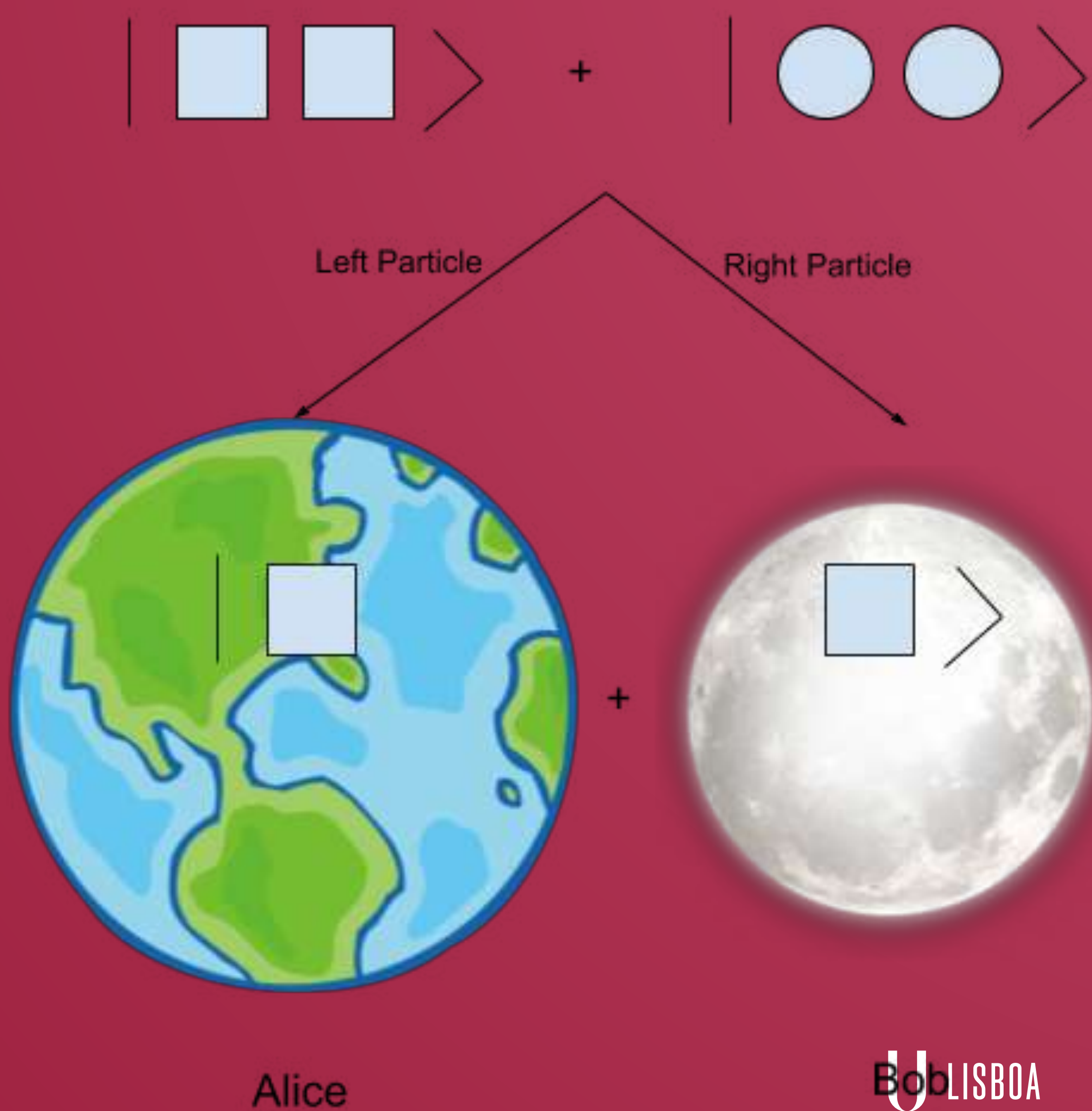
QUANTUM ENTANGLEMENT

LASIGE reliable software systems

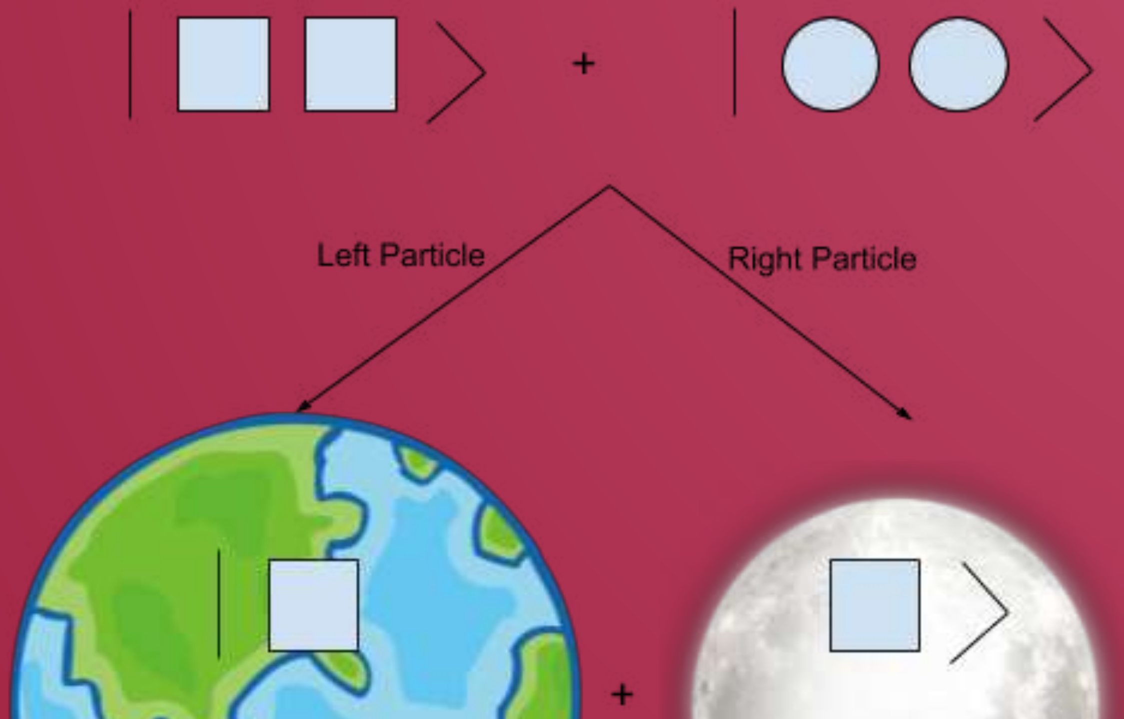


ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

QUANTUM ENTANGLEMENT



QUANTUM ENTANGLEMENT



Entanglement is a set of particles for which we can not write the states as a direct product of single classical particles, (e.g. $|00\rangle + |11\rangle \neq (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle$ for all a, b, c, d) – This does not exist in classical world.

Alice

Bob

QUANTUM VS CLASSICAL

LASIGE reliable software systems

	Classical	Quantum
Unity of information	Bit, 0 or 1	Qubit, i.e, a linear combination of |0> and |1>
Copy	Yes	Only classical information
Entanglement	No, any two bit can exist separately with a meaning	Yes, there are 2 particles states for which we can not write the states as a direct product of single classical particles, (e.g. |00> + |11> != (a|0>+b|1>) ⊗(c|0>+d|1>, for all a, b, c, d)
Evolution	Logical gates (may be irreversible)	Quantum logic gates (unitary transformations that are always reversible)
Computational power	Turing machines	Turing machines
Non-local effects	No	Yes
Communication faster than light	No	No

POWER OF QUANTUM - AN EXAMPLE

LASIGE reliable software systems

- Consider a function f:{0,1} → {0,1}. How many queries do you need to know whether f is constant?

ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

POWER OF QUANTUM - AN EXAMPLE

LASIGE reliable software systems

- Consider a function f:{0,1} → {0,1}. How many queries do you need to know whether f is constant?

  - Depends:
    - Classically –
    - Quantumly –

POWER OF QUANTUM - AN EXAMPLE

- Consider a function f:{0,1} → {0,1}. How many queries do you need to know whether f is constant?
  - Depends:
    - Classically – 2
    - Quantumly – 1

POWER OF QUANTUM - AN EXAMPLE

- Consider a function f:{0,1} → {0,1}. How many queries do you need to know whether f is constant?
  - Depends:
    - Classically – 2
    - Quantumly – 1
- Consider a function $f:\{0,1\}^n \rightarrow \{0,1\}$ that is either constant or balanced. How many queries do you need to know whether f is constant or balanced?
    - Classically –
    - Quantumly –

POWER OF QUANTUM - AN EXAMPLE

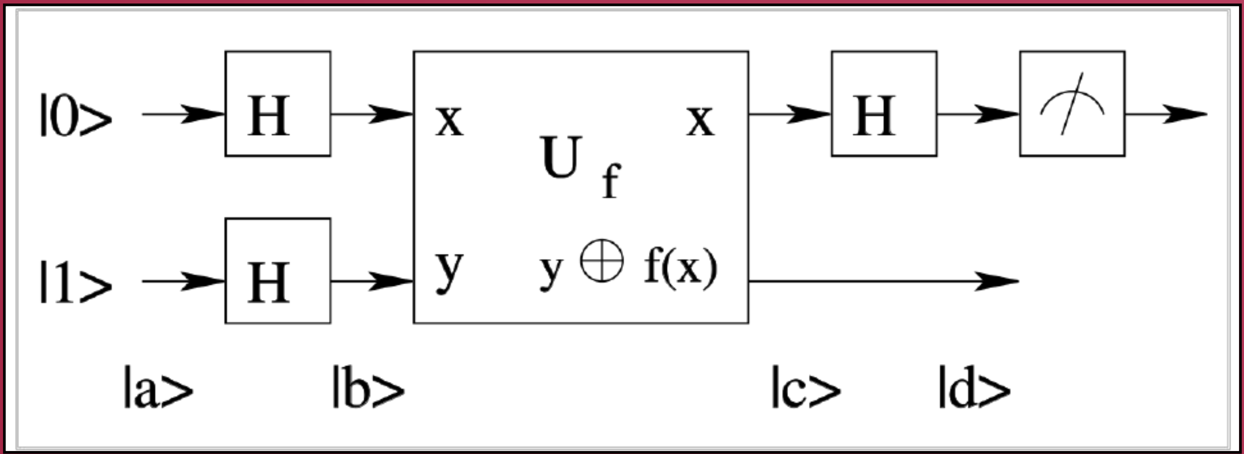
LASIGE reliable software systems

- Consider a function f:{0,1} → {0,1}. How many queries do you need to know whether f is constant?
  - Depends:
    - Classically – 2
    - Quantumly – 1
- Consider a function f:$\{0,1\}^n$ → {0,1} that is either constant or balanced. How many queries do you need to know whether f is constant or balanced?
    - Classically – $2^{n-1} + 1$
    - Quantumly – 1

U LISBOA | Ciências ULisboa | FCT Fundação para a Ciência e a Tecnologia

POWER OF QUANTUM - AN EXAMPLE– DEUTSCH ALGORITHM

- Consider a function f:{0,1} → {0,1}. Is f constant?



single query but answer in superposition

$|a\rangle = |0\rangle|1\rangle$ → $|b\rangle = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle)$

→ $|c\rangle = \frac{1}{2} (|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)$

$= \frac{1}{2} ((-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle) + (-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle)$

$= \frac{1}{2} (|0\rangle + (-1)^{f(0)\oplus f(1)} |1\rangle)(|0\rangle - |1\rangle)$

→ $|d\rangle = \frac{1}{2} |0\rangle (|0\rangle - |1\rangle)$ if f is constant or

$|d\rangle = \frac{1}{2} |1\rangle (|0\rangle - |1\rangle)$ if f is balance

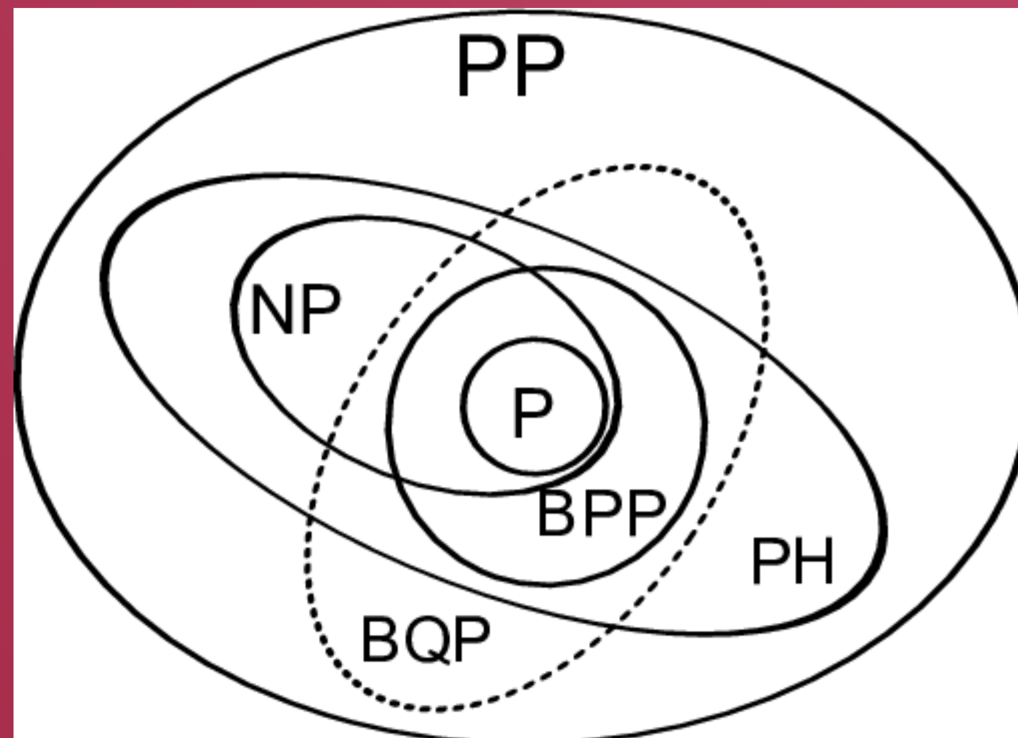
WHAT BOOST CAN WE HAVE?

WHAT BOOST CAN WE HAVE?

- Depends:
  - If it is a promised problem, we can have an exponential boost when compared with best classical algorithms:
    - Deutch-Jozsa,
    - Bernstein,
    - Shor, etc…
  - In general (not proven yet), the boost is only polynomial:
    - Grover’s search algorithm -- quadratic speedup
    - Recommendation systems algorithms (2018) – polynomial speedup.
  - If P = BQP then BPP = BQP

QUANTUM ON THE "ZOO"

- BQP PP proved by Adleman et al in 97
- Best result known: BQP $\subseteq$ AWPP (almost wide PP, NP machine with negligible error) proved in 98
- There exists an oracle such that $BQP^{O} \not\subset PH^{O}$ Raz Tal 18



QUANTUM DEVICES AVAILABLE

LASIGE reliable software systems

- Truly random bit generator!

- Quantum Cryptography Platform

- Quantum key generator

- Quantum computer – IBM Q

U LISBOA | Ciências ULisboa | FCT Fundação para a Ciência e a Tecnologia

HOW MANY QUBITS DO QUANTUM COMPUTER HANDLE?

LASIGE reliable software systems

- Mar/2018:
  - Alibaba: 11 qubits cloud,
  - Google: 72 qubits (but usable only 49 with good accuracy),
- Feb/2018:
  - IBM: 50 qubits, 20 qubits cloud,
  - Intel: 49 qubits,
  - Google: 50 qubits,
  - D-Wave 2000 qubits (but their chips aren't in the same category that everyone else's efforts, and their performance also leaves many unanswered questions).

- In theory we can factor numbers up to 70 digits! (the record of largest factored number is 291311 – only 6 digits).

ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

USES OF QUANTUM COMPUTATION

- Optimization
- System simulation
- Machine learning
- Material simulation
- Computational Chemical/Microbiology
- Circuit, Software, and System Fault Simulation
- Code breaking
- Cryptography

EXHIBIT 2 | Multiple Potential Use Cases for Quantum Computing Exist Across Sectors

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)
High-tech	• Machine learning and artificial intelligence, such as neural networks • Search • Bidding strategies for advertisements • Cybersecurity • Online and product marketing • Software verification and validation	IBM, Telstra, Alibaba, Baidu, Google, Samsung, Microsoft
Industrial goods	• Logistics: scheduling, planning, product distribution, routing • Automotive: traffic simulation, e-charging station and parking search, autonomous driving • Semiconductors: manufacturing, such as chip layout optimization • Aerospace: R&D and manufacturing, such as fault-analysis, stronger polymers for airplanes • Material science: effective catalytic converters for cars, battery cell research, more-efficient materials for solar cells, and property engineering uses such as OLEDS	Airbus, BMW, NASA, Volkswagen, Northrop Grumman, Lockheed Martin, Daimler, Honeywell, Raytheon, Bosch
Chemistry and Pharma	• Catalyst and enzyme design, such as nitrogenase • Pharmaceuticals R&D, such as faster drug discovery • Bioinformatics, such as genomics • Patient diagnostics for health care, such as improved diagnostic capability for MRI	BASF, JSR, Biogen, DuPont, Dow Chemical, Amgen
Finance	• Trading strategies • Portfolio optimization • Asset pricing • Risk analysis • Fraud detection • Market simulation	J.P. Morgan, Barclays, Commonwealth Bank, Goldman Sachs
Energy	• Network design • Energy distribution • Oil well optimization	Dubai Electricity & Water Authority, BP

Source: BCG analysis.

CRYPTOGRAPHIC APPLICATIONS

LASIGE reliable software systems

- Why is quantum technologies needed in crypto?
  - Speedup of computation and communication;
  - Security does not depend on computational hardness assumptions but relies on the principles of quantum mechanics;
  - More communication efficient protocols (like BB84);
  - BC cannot be theoretical information secure classically;
  - BC, in principle, could be theoretical information secure in the quantum realm;
  - BC can be constructed from OT but the other way around requires (perfectly secure) BC;

- Problems
  - Cost of set up;
  - Distance of quantum apparatus (up to near 100 km without repeaters);
  - Stability of quantum memories;

U LISBOA | Ciências ULisboa | FCT Fundação para a Ciência e a Tecnologia

MAJOR RESULTS AND MILESTONES

- Quantum cryptography
  - Key exchange: Single photon sources (BB84, E91);
  - Privacy: BC, OT, Weak coin flipping
- Post quantum cryptography (based on computational hard assumption, not of laws of physics)
  - McEliece – syndrome decoding problem
  - NTRU, LWE – shortest vector problem and learning with errors
  - Supersingular elliptic curves (isogenies) – hardness of finding the isogenies of an EC

OBLIVIOUS TRANSFER AND COMMITMENTS – WHY?

- They are really simple to understand;
- They are the basics of the basics, meaning that, from them we can construct all the other SMC protocols (Yao);
- All privacy functionalities can be reduced to implementing oblivious transfer (OT) (Kilian);
- Perfect bit commitment is possible under special relativity – impossibility of faster than light speed communication. (Kent)
- Using classical crypto one can perform at around 360 OTb/s!
  - So to cipher a text using AES which needs around 1000 k OTb, would take around 50 minutes!
- To make more OT per second classically one has to reduce OT security, but not necessarily in quantum!
- Shor's can break Rabin's OT.

OBLIVIOUS TRANSFER AND COMMITMENT EXPLAINED

LASIGE reliable software systems

- Oblivious transfer:

  - Two agents Alice and Bob: Alice wants to share a secret with Bob such that
    - 1) Bob will receive it with probability ½;
    - 2) Alice with not be able to know whether Bob got it or not;

OBLIVIOUS TRANSFER AND COMMITMENT EXPLAINED

LASIGE reliable software systems

- Oblivious transfer:
  - Two agents Alice and Bob: Alice wants to share a secret with Bob such that
    - 1) Bob will receive it with probability ½;
    - 2) Alice with not be able to know whether Bob got it or not;
- Bit Commitment
  - Two agents Alice and Bob: They want to play coin tosses over the telephone
    - 1) Alice has to be binded to the value chosen (she cannot change it later)
    - 2) Bob cannot distinguish a commitment to 0 from a commitment to 1 (concealing)

CLASSICAL APPROACH

LASIGE reliable software systems

- Oblivious transfer (Rabin's)

  Consider N = pq and e co prime with Phi(N).

  Alice computes m^e mod N and sends N, m^e mod N and e to Bob

  Bob pick x and sends x^2 mod N to Alice.

  Alice replies with y such that $y^2 = x^2$. If y != +/- x Bob recovers m by factoring N.

  By the CRT happens with probability ½

- Bit commitment

  Consider a one way function f (easy to compute and hard to invert). Examples: OWF based of factoring or Sha256!

  In the commitment phase Alice computes f (xb) for a random string x and her bit b;

  In the opening she reveals x and b to Bob.

U LISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

BAD NEWS, THEN WHAT?

- No unconditionally secure (bit) Oblivious Transfer protocol nor Bit Commitment protocols are possible – No-go Theorems (Mayers, Lo and Chau 98)

- We can construct String Commitments and String Oblivious transfer or impose (realistic) restrictions on the adversaries for single bit versions:
  - Relativistic effects;
  - Noisy quantum memories;
  - Bounded entanglement;
  - Semi-quantum agents;
  - Trusted third-parties;

A SIMPLE PROTOCOL FOR A PRACTICAL BC – THE FUNCTIONALITY

LASIGE reliable software systems

Functionality $\mathcal{F}_{\mathrm{COM}}$

Parameters:

- Parties Alice and Bob.
- Size k of the committed value.

1) Upon receiving an input (*commit, x*) from Alice, if no value has previously been committed, output the message (*committed*) to Bob.
2) Upon receiving the input (*open*) from Alice, if a value x has previously been committed, output the message (*open, x*) to Bob, and halt.

Figure 1: Commitment functionality.

Functionality $\mathcal{F}_{\mathrm{AQB}}$

Parameters:

- Parties Alice and Bob.
- Security parameter m.
- Injective function $\mathcal{C} : \{0,1\}^{m/2} \to \{0,1\}^m$, such that $\mathcal{C}(s) = s.f(s)$, where f is an (almost) perfectly non-linear function.
- Time interval Δt.
- Set $\mathcal{B} = \{(|e_0^s\rangle, |e_1^s\rangle)\}_{s\in\{0,1\}^{m/2}}$ of bases of $\mathbb{C}^2$, such that $\forall s\ \exists \bar{s}\ (|e_0^s\rangle, |e_1^s\rangle) = (|e_1^{\bar{s}}\rangle, |e_0^{\bar{s}}\rangle)$.

Upon activation, $\mathcal{F}_{\mathrm{AQB}}$ sets the time index $\tau = 1$ and repeats the following steps at regular time intervals Δt.

1) Sample random $s \in \{0,1\}^{m/2}$, $\ell \in \{0,1\}^m$, and bit j.
2) Compute $\mathcal{C}(s)$.
3) Output $(\mathcal{C}(s) \oplus \ell, j, \tau)$ to Alice and $(\ell, |e_j^s\rangle, \tau)$ to Bob.
4) Increase τ by 1.

Figure 2: Assymetric quantum beamer functionality.

Fundação para a Ciência e a Tecnologia

A SIMPLE PROTOCOL FOR A PRACTICAL BC

LASIGE reliable software systems

Protocol $\pi_{\text{BC}}^{\text{AQB}}$

Parameters: A functionality $\mathcal{F}_{\text{AQB}}$ with security parameter m, basis set $\mathcal{B}$.

Parties: The sender Alice and the receiver Bob.

Setup phase

1) Alice chooses a time index τ and sends it to Bob. Then, Alice and Bob record the outputs $(\mathcal{C}(s) \oplus \ell, j, \tau)$ and $(\ell, |e_j^s\rangle, \tau)$, respectively, sent by $\mathcal{F}_{\text{AQB}}$.

Commit phase

Inputs: Alice gets a bit b.

2) Alice commits the bit b to Bob by sending him $c = b \oplus j$.
3) After receiving c from Alice, Bob outputs the message *receipt*.

Open phase

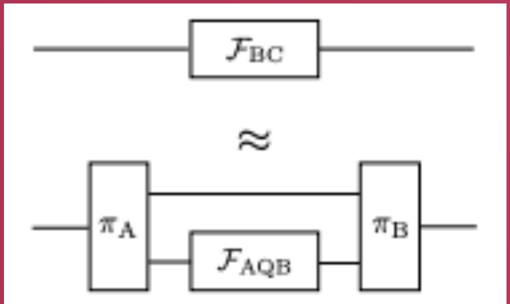
Inputs: Alice gets the message *open*.

4) Alice sends $q = \mathcal{C}(s) \oplus \ell$ to Bob.
5) If $q \oplus \ell \notin \text{Im}(\mathcal{C})$, Bob outputs *error*. Otherwise, he computes $s = \mathcal{C}^{-1}(q \oplus \ell)$, measures his qubit $|e_j^s\rangle$ in the basis $(|e_0^s\rangle, |e_1^s\rangle)$ to obtain j, and outputs $b = c \oplus j$.

Figure 3: Bit commitment protocol $\pi_{\text{BC}}^{\text{AQB}}$ using the functionality $\mathcal{F}_{\text{AQB}}$.

U LISBOA   Ciências ULisboa   FCT Fundação para a Ciência e a Tecnologia

SKETCH OF THE PROOF

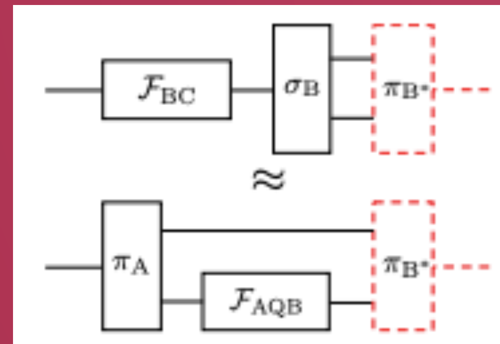


- Soundness:

Because the value of *j* is fixed during the setup phase, when Alice sends $c=b\oplus j$, she fixes her commitment to b. Measuring $|e_j^i\rangle$ in the basis B_i is guaranteed to output j. Therefore, Bob always obtains b by taking $c\oplus j$.

SKETCH OF THE PROOF

LASIGE reliable software systems



- Concealing:

Consider the following program for the converter s_B. During the setup phase, s_B simulates F_{AQB} to generate the values s, C(s), \ell, j and the qubit $|e_j^i>$ then sends (\ell, $|e_j^i>$) to the adversary. In the commit phase, upon receiving *commit* from F_{BC}, it sends c'=j to the adversary.

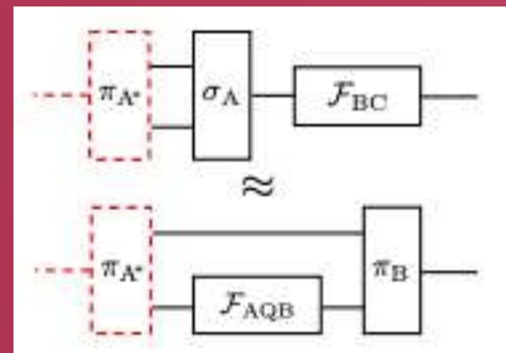
During the open phase, after receiving (open, b) from F_{BC}, if b=0 it sends q=C(s)⊕\ell to the adversary, otherwise q' = C(~s)⊕\ell.

The concealing property comes by noting that the behavior of s_B is the same regardless of the bit that was sent to F_{AQB}, hence there is no algorithm Pi_{B^*} that can guess the committed bit with probability greater than ½.

U LISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

SKETCH OF THE PROOF

LASIGE reliable software systems



- Binding

Consider the following program for the converter s_A. During the setup phase, s_A simulates F_{AQB} to generate the values s, C(s), \ell, j and the qubit $|e_j^i>$. It then sends (q=C(s)⊕\ell, j) to the adversary. During the commit phase, upon receiving a bit c' from the adversary, it computes b=c' ⊕ j and outputs (commit, b) to F_{BC}. During the opening phase, upon receiving q' from the adversary, if q'=q it outputs (open) to F_{BC}.

Bob outputs error whenever q' sent by Alice is such that q'⊕\ell \notin Im(C). From the soundness property we know that when q=q' Bob opens b=c'⊕j. We are interested in the case when q' \neq q and q'⊕\ell \in Im(C). Because f(s) is injective and almost perfectly non-linear, finding such q' given q is equivalent to finding s given C(s)⊕\ell, which the adversary can do only with negligible probability.

THE QUANTUM TIMELINE

LASIGE reliable software systems

- https://en.wikipedia.org/wiki/Timeline_of_quantum_computing

ULISBOA Ciências ULisboa FCT Fundação para a Ciência e a Tecnologia

CONCLUSIONS

- Quantum resources can in principle attain rates of OT impossible to perform with classical crypto;
- Large scale privacy protocols, like private data mining can arise from this scenario;
- Future work: use of continuous variables (and the Heisenberg uncertainty principle) to obtain fast OT, other crypto functionalities, authentication (using entanglement), non-repudiation, verifiable secret sharing, e-voting.

SO, WHAT'S NEXT

- At this time we have on going on crypto:
  - Practical implementation and realization of a semi-quantum protocol for QKD with classical Alice and Bob and a fully quantum server;
  - Quantum key distribution with quantum walks;
  - OT based on BC with collision resilient hash functions;
  - Quantum contract signing with entangled pairs;
  - BC based on monogamy of entanglement;
  - Quantum resilient cryptosystems based on McEliece, Goppa codes and NTRU.
- Other things ongoing on quantum:
  - Proof of Brudno's theorem with QKC;
  - New proposal based on QKC to "quantify" quantum correlations;
  - Realizing quantum zero knowledge with an individual approach;

LAST MINUTE

- Special talk: **Quantum Internet**

  Speaker: Stephanie Wehner (QuTech, Delft University of Technology)

  Date: Tuesday 14 May 2019
  Time: 17:00
  Venue: Sala 1, Fundação Calouste Gulbenkian, Lisbon